

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division**

MICHAEL FORREST KOVACH,       )  
  )  
      Petitioner,                    )  
  )  
v.                                        )  
  )  
HAROLD W. CLARKE,                )  
  )  
      Respondent.                  )

Civil Action No. 3:22-cv-175–HEH

**MEMORANDUM OPINION**  
**(Granting Respondent’s Amended Motion to Dismiss)**

Michael Forrest Kovach (“Kovach”), a Virginia inmate proceeding with counsel, filed this petition for a writ of habeas corpus under 28 U.S.C. § 2254 (“§ 2254 Petition,” ECF No. 1) challenging his convictions in the Circuit Court for Westmoreland County (“Circuit Court”). Kovach contends that he is entitled to relief on the following ground:

The state court erred when it failed to find that trial counsel was ineffective under the Sixth Amendment of the United States Constitution for failing to sufficiently investigate, consult with their experts, and challenge the charges of distribution [of child pornography] on the basis that the Commonwealth failed to prove that Kovach had the requisite *mens rea* for distribution.

(ECF No. 1 at 13 (as paginated by CM/ECF).) Respondent has moved to dismiss. (ECF No. 10.) Kovach has replied. (ECF No. 14.) For the reasons that follow, the Amended Motion to Dismiss will be granted.

## I. PROCEDURAL HISTORY

Following a bench trial, the Circuit Court convicted Kovach of one count of possession of child pornography, two counts of possession of child pornography, second or subsequent offense, and three counts of distribution of child pornography. (ECF No. 1–1 at 22.) Kovach appealed his convictions on the ground that the evidence was insufficient to prove his guilt. (*Id.* at 23.)

The Court of Appeals of Virginia provided the following relevant summary of the evidence and the proceeding in the Circuit Court:

On November 19, 2013, Special Agent Mike Jedrey of the Virginia State Police began investigating an IP address suspected of distributing child pornography. The IP address provided him with a file list containing terms of child exploitation. From this list, Special Agent Jedrey attempted to download some of the files to verify the content. He was able to download the files using a peer-to-peer sharing platform designed to facilitate file sharing between computers. Special Agent Jedrey later traced the IP address to appellant because the address was registered to appellant's residence.

On March 5, 2014, Special Agent Jedrey, along with several other officers, executed a search warrant of appellant's home. Nine items were seized including a Dell Dimension 2400 Tower, an iPhone, two SD cards, three laptops, an external hard disc drive, and a large black custom computer desk top tower.

On the same day, Special Agent Jedrey interviewed appellant. Appellant stated that only he and his sons lived in the house and that he monitored the computers very carefully, controlling what information his sons could access. He also indicated that he downloaded peer-to-peer sharing software, Shareaza, on his computer and admitted to downloading adult pornography. Appellant also stated that while he was downloading these files, he viewed child pornography on a zip file<sup>1</sup> that he downloaded using Shareaza.

---

<sup>1</sup> A zip file is downloaded by a computer user and allows multiple pictures, videos, or any other type of file to be contained within a compressed file to provide space on a computer and make transmission more efficient.

At trial, Special Agent Jedrey testified about the files that came from the IP address registered to appellant's home which Special Agent Jedrey downloaded using peer-to-peer sharing programs. As part of his investigation, Special Agent Jedrey testified that for several months he would download files that he suspected of being child pornography. Some of these images were found on a zip file on appellant's desktop and a SD card.<sup>2</sup> [Special Agent Jedrey used] the files he downloaded . . . to obtain a search warrant for appellant's home.

Thomas Heflin, an expert in the field of digital forensic examination, testified about what the investigators found on the items seized from appellant's house. Child pornography was found on a laptop, the desktop computer, and a SD card. The child pornography was found in the unallocated space<sup>3</sup> on the desktop and in the thumb cache<sup>4</sup> on the laptop. Heflin testified that there were videos on the SD card depicting child pornography, which the Commonwealth played at trial. Heflin also testified that when he examined the desktop the user name for the peer-to-peer sharing program installed on the computer was "Mike."

Lawrence Daniel, an expert in forensic examination, testified that he could not tell from examining the SD card whether it had been accessed by other computers. Daniel also stated that he did not find any link file from the SD card on the laptop or the desktop, which would have appeared if a link had been opened on either device from the SD card. Further, Daniel testified that the only pictures found on the desktop and laptop computer were in the unallocated space or the thumb cache. Both the unallocated space and the thumb cache require special software to gain access to them; there was no evidence of any such programs on either the laptop or the desktop. Daniel testified that because the globally unique identifier ("GUID") number, which Special Agent Jedrey found while downloading suspicious files using the peer-to-peer sharing program, matched appellant's desktop, it followed that the child pornography came from appellant's computer.

At the close of the Commonwealth's case, appellant moved to strike the evidence on each charge. Appellant argued that the evidence presented

---

<sup>2</sup> A SD card is a memory card that stores files and can be inserted into a computer.

<sup>3</sup> Unallocated space is an area of the computer where files that users have viewed will be stored, even if they are deleted, until they are eventually overwritten. Files found in the unallocated space on a computer could not be accessed by a user without some specialized software or program.

<sup>4</sup> A thumb cache is a Microsoft Windows database designed to store smaller versions of images that a computer user looks at in Windows Explorer. Thumb cache images on a computer cannot be accessed by a user without some specialized software or program.

by the Commonwealth was insufficient to support the child pornography possession and distribution charges against him. Appellant argued that the Commonwealth could not prove that appellant knowingly possessed child pornography because the only pictures found on the desktop and the laptop were in places the appellant could not access, specifically the unallocated space and the thumb cache. Appellant further argued that people who have SD cards do not necessarily know what is on them. Appellant stated that there was no way to prove appellant ever accessed, acquired, or viewed anything on the SD card containing child pornography.

In his motion to strike, appellant also argued that there was no way to prove that the people in the videos were children. He further stated that there was no way for the trial court to know which picture or video corresponded with each indictment. Ultimately, the trial court denied appellant's motion to strike.

The trial court found appellant guilty of possession of child pornography, two counts of possession of child pornography as a second or subsequent offense, distribution of child pornography, and three counts of distribution of child pornography as a second or subsequent offense. While the trial court admitted that it was not trying to limit the possession charges to a particular exhibit, it did state that the first possession conviction was based on evidence found in the thumb cache on the desktop, the second possession conviction was based on evidence found in a Shareaza "collection" zip file, and the third possession conviction was based on evidence found in the unallocated space on the laptop. The first distribution conviction was based on one photo that Special Agent Jedrey downloaded on November 21, 2013. The second distribution conviction was based upon the evidence of all the other photographs Special Agent Jedrey downloaded on November 21, 2013. The third distribution conviction was based on all the images Special Agent Jedrey downloaded on December 9, 2013. The fourth distribution conviction was based on all the images Special Agent Jedrey downloaded on November 19, 2013. The trial court sentenced appellant to a total of forty years in prison, with twenty-five years suspended. This appeal followed.

*Kovach v. Commonwealth*, No. 2013–15–2, 2016 WL 7094215, at \*1–2 (Va. Ct. App.

Dec. 6, 2016).

The Court of Appeals of Virginia affirmed in part and reversed in part. *Id.* at \*1.

With respect to the possession of child pornography charges, the Court of Appeals stated:

Code § 18.2-374.1:1(A) states that “[a]ny person who knowingly possesses child pornography is guilty of a Class 6 felony.” To convict appellant of possession of child pornography, the Commonwealth had to prove appellant “was aware of the presence and character of the [contraband] and that he intentionally and consciously possessed [it].” *Merritt v. Commonwealth*, 55 Va. App. 719, 733, 689 S.E.2d 757, 764 (2010) (quoting *Castaneda v. Commonwealth*, 7 Va. App. 574, 583, 376 S.E.2d 82, 87 (1989)); see also *Terlecki v. Commonwealth*, 65 Va. App. 13, 24–25, 772 S.E.2d 777, 782–83 (2015) (holding that possession of child pornography may be analyzed under principles of constructive possession).

“Possession can be proven ‘by showing either actual or constructive possession.’” *Merritt*, 55 Va. App. at 733, 689 S.E.2d at 764 (quoting *Birdsong v. Commonwealth*, 37 Va. App. 603, 607, 560 S.E.2d 468, 470 (2002)). “Proof of constructive possession necessarily rests on circumstantial evidence; thus, ‘all necessary circumstances proved must be consistent with guilt and inconsistent with innocence and exclude every reasonable hypothesis of innocence.’” *Id.* (quoting *Burchette v. Commonwealth*, 15 Va. App. 432, 435, 425 S.E.2d 81, 83 (1992)). When proving constructive possession of contraband, as in this case, “the Commonwealth must point to evidence of acts, statements, or conduct of the accused or other facts or circumstances which tend to show that [appellant] was aware of both the presence and character of the [contraband] and that it was subject to his dominion and control.” *Powers v. Commonwealth*, 227 Va. 474, 476, 316 S.E.2d 739, 740 (1984) (citing *Eckhart v. Commonwealth*, 222 Va. 447, 450, 281 S.E.2d 853, 855 (1981)).

In this case, appellant argues that the Commonwealth’s evidence was insufficient for the trial court to convict him of the possession charges because there was no evidence that appellant had knowledge of what was on his desktop or laptop, in the unallocated space or the thumb cache. Appellant also argues that the Commonwealth did not provide evidence to support the trial court’s finding that he had knowing possession or dominion and control over the SD card found by the police.<sup>5</sup>

In *Kobman v. Commonwealth*, 65 Va. App. 304, 307–08, 777 S.E.2d 565, 567 (2015), this Court found that the mere presence of contraband in the unallocated space of a computer does not establish knowing possession of the contraband because the material in the unallocated space cannot be accessed or seen without forensic software. Likewise, in the present case,

---

<sup>5</sup> Appellant did not provide a substantial argument about the evidence found on the desktop in the Shareaza “collection” zip file which is what the trial court considered in convicting him of the second possession charge, instead appellant focused on the SD card.

investigators found images in the unallocated space of appellant's desktop, but because no forensic software was found on the computer allowing access to the material appellant could not be found to possess the contraband. Therefore, the trial court erred in denying the motion to strike because no evidence established that appellant had knowledge, dominion, or control of the photographs found in the unallocated space.<sup>6</sup>

The trial court also erred by denying the motion to strike as it related to the possession charges for images in the thumb cache. Based on Daniel's expert testimony, special software is required to access the thumb cache, similar to that necessary for accessing the unallocated space. Pursuant to *Kobman*, when special software is required to access part of a computer, and that special software is not present, the recovered evidence by itself does not establish criminal liability. 65 Va. App. at 307–08, 777 S.E.2d at 567. In this case, there was no evidence that appellant had the software on his laptop that was necessary to access the thumb cache.

For the remaining possession charge, based on the evidence found on the desktop in the Shareaza "collection" zip file, the Commonwealth advances a theory of constructive possession of the contraband. As previously stated, "the Commonwealth must point to evidence of acts, statements, or conduct of the accused or other facts or circumstances which tend to show that the [appellant] was aware of both the presence and character of the [contraband] and that it was subject to his dominion and control." *Powers*, 227 Va. at 474, 316 S.E.2d at 739. "Ownership or occupancy of the premises on which the contraband was found is a circumstance probative for possession." *Archer v. Commonwealth*, 26 Va. App. 1, 12, 492 S.E.2d 826, 832 (1997). In the present case, the police recovered images from the desktop in a Shareaza "collection" zip file. Special Agent Jedrey testified that these images were accessible to users without any special programs. In addition, appellant admitted to Special Agent Jedrey that he saw an image of child pornography on a zip file. This evidence, coupled with the facts which bolster the finding that appellant had control over the desktop, the images located in the zip file which were under the user name "Mike," and because the zip file had recently been opened on the desktop, lead to the conclusion that appellant knew the images were on the desktop and were under his dominion and control. Viewing the evidence in the light most favorable to the Commonwealth, the trial court's ruling on the motion to strike as it related to the evidence found on the desktop in the

---

<sup>6</sup> The Commonwealth concedes this point on brief, citing *Kobman*. While this Court is not obligated to follow concessions of law by the Commonwealth, this concession of law is an appropriate recognition of controlling principles in this matter. See *Logan v. Commonwealth*, 47 Va. App. 168, 172, 622 S.E.2d 771, 773 (2005) (en banc).



Shareaza “collection” zip file was not plainly wrong or without evidence to support it.

With regard to the pictures found on the SD card, the trial court did not specifically base any conviction on the evidence found there but it still acknowledged in its ruling that when it assigned a particular exhibit to a charge “it was not trying to limit it to just those particular exhibits.” The trial court also stated that “from the beginning, the case has been about essentially the SD drive and the two computers.” The Commonwealth again offers a theory of constructive possession of the contraband. The Commonwealth argues that several different “acts, statements, [and certain] conduct” of appellant would lead a factfinder to conclude that appellant possessed the child pornography recovered by the police on the SD card. *See Powers*, 227 Va. at 474, 316 S.E.2d at 739.

These facts included that the SD card was found in appellant’s hamper in his bedroom. Next, appellant admitted that he controlled the electronic devices in his house and stated that he was the “dragon” between his sons and the computers, monitoring their use of electronics. Appellant admitted that sometimes suspect images and videos appeared when he was trying to download adult pornography. Lastly, several of the videos that Special Agent Jedrey obtained while he was using peer-to-peer sharing software were also found on the SD card. Viewing the evidence in the light most favorable to the Commonwealth, the trial court’s ruling on the motion to strike as it related to the possession charges from the SD card was not plainly wrong or without evidence to support it.

In summary, we conclude that the trial court erred when it found that the child pornography found in the unallocated space on the desktop and in the thumb cache on the laptop established appellant’s guilt because special forensic software programs and training were necessary to access these images. Thus, we reverse the two possession of child pornography second or subsequent convictions based on the files found in the unallocated space and thumb cache. We affirm the possession of child pornography conviction based on the evidence found in the “collection” zip file downloaded using Shareaza.

*Id.* at \*3–5 (alterations in original).

The Court of Appeals also affirmed Kovach’s convictions of distribution of child pornography. *Id.* at \*5. The Court of Appeals stated in pertinent part:

Appellant argues that he should not have been convicted of distribution of child pornography because the evidence was insufficient to prove that he

intentionally shared child pornography or was the person responsible for sharing it.

In *Kelley v. Commonwealth*, 289 Va. 463, 469, 771 S.E.2d 672, 674–75 (2015), the Supreme Court of Virginia held that because the appellant chose to download peer-to-peer sharing software onto his laptop, he voluntarily participated in peer-to-peer sharing of child pornography. The Court also found that appellant knew how the peer-to-peer sharing software worked and knew that the software was capable of sharing files with other users, regardless of whether appellant intended to share the files or if they were just put into a shared folder as a default option by the program. *Id.*

Similarly, in this case, appellant knowingly downloaded and used the peer-to-peer sharing software on his desktop. Appellant admitted to downloading movies and adult pornography using Shareaza, showing he knew how to use the software. Appellant also admitted that he had accidentally downloaded child pornography in the past. It was reasonable for the factfinder to conclude that appellant should have known that the software had the ability to share files with other users. Appellant's assertion that he did not know that the sharing feature was operating is insignificant. Furthermore, the trial court did not find appellant's statements to Special Agent Jedrey, with respect to his awareness of or intention to share pornographic image files, credible.

Moreover, a GUID number that Special Agent Jedrey captured while downloading photographs onto his computer during his investigation was a number generated during the installation of Shareaza on appellant's desktop. Daniel testified that because this GUID number matched appellant's desktop, Special Agent Jedrey downloaded the child pornography from appellant's computer. Finally, several of the videos that Special Agent Jedrey obtained while he was using peer-to-peer sharing software were also found on the SD card in appellant's hamper.

Based on the facts and circumstances presented to the trial court, we hold that the trial court was not plainly wrong in denying appellant's motion to strike the charges of distribution of child pornography. Accordingly, we affirm appellant's conviction of distribution of child pornography in violation of Code § 18.2–374.1:1(C), and his three distribution of child pornography second or subsequent offenses in violation of Code § 18.2–374.1:1(C).

*Id.* The Supreme Court of Virginia refused Kovach's petition for appeal. (ECF No. 12-6 at 1.)



On June 5, 2018, Kovach, by counsel, filed a petition for a writ of habeas corpus with the Circuit Court wherein he raised the same claim that he raises in his federal habeas petition. (ECF No. 12-7 at 1.)<sup>7</sup> The Circuit Court denied the petition. (ECF No. 1-1 at 24.) Kovach appealed. The Supreme Court of Virginia refused the petition for appeal. (ECF No. 12-11.)

## **II. APPLICABLE CONSTRAINTS UPON FEDERAL HABEAS REVIEW**

To obtain federal habeas relief, at a minimum, a petitioner must demonstrate that he is “in custody in violation of the Constitution or laws or treaties of the United States.” 28 U.S.C. § 2254(a). The Antiterrorism and Effective Death Penalty Act of 1996 (“AEDPA”) further circumscribes this Court’s authority to grant relief by way of a writ of habeas corpus. Specifically, “[s]tate court factual determinations are presumed to be correct and may be rebutted only by clear and convincing evidence.” *Gray v. Branker*, 529 F.3d 220, 228 (4th Cir. 2008) (citing 28 U.S.C. § 2254(e)(1)). Additionally, under 28 U.S.C. § 2254(d), a federal court may not grant a writ of habeas corpus based on any claim that was adjudicated on the merits in state court unless the adjudicated claim:

- (1) resulted in a decision that was contrary to, or involved an unreasonable application of, clearly established Federal law, as determined by the Supreme Court of the United States; or
- (2) resulted in a decision that was based on an unreasonable determination of the facts in light of the evidence presented in the State court proceeding.

28 U.S.C. § 2254(d). The Supreme Court has emphasized that the question “is not whether a federal court believes the state court’s determination was incorrect but whether

---

<sup>7</sup> The Court employs the pagination assigned by the CM/ECF docketing system.

that determination was unreasonable—a substantially higher threshold.” *Schriro v. Landrigan*, 550 U.S. 465, 473 (2007) (citing *Williams v. Taylor*, 529 U.S. 362, 410 (2000)). Given the foregoing restrictions, the findings of the Circuit Court figure prominently in this Court’s opinion.

### III. ANALYSIS

To demonstrate ineffective assistance of counsel, a convicted defendant must first show that counsel’s representation was deficient, and, second, that the deficient performance prejudiced the defense. *Strickland v. Washington*, 466 U.S. 668, 687 (1984). To satisfy the deficient performance prong of *Strickland*, a convicted defendant must overcome the “‘strong presumption’ that counsel’s strategy and tactics fall ‘within the wide range of reasonable professional assistance.’” *Burch v. Corcoran*, 273 F.3d 577, 588 (4th Cir. 2001) (quoting *Strickland*, 466 U.S. at 689). The prejudice component requires a convicted defendant to “show that there is a reasonable probability that, but for counsel’s unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome.” *Strickland*, 466 U.S. at 694. In analyzing ineffective assistance of counsel claims, the Court need not determine whether counsel performed deficiently if the claim is readily dismissed for lack of prejudice. *Id.* at 697.

Kovach argues that,

trial counsel was ineffective for failing to investigate, consult with their expert[s] and challenge the charges of distribution based on the lack of any evidence at all that Kovach intended or knew that the files law enforcement downloaded were available for downloading — that is, Kovach never had the requisite mens rea for distribution.

(ECF No. 1 ¶ 45.)

In a thorough and detailed opinion, the Circuit Court made the following pertinent findings:

Petitioner argues that his trial counsel were ineffective because they failed to sufficiently investigate and consult with their experts; had they done so, Petitioner maintains that he could have prevailed on the charges of distribution of child pornography “on the basis that the Commonwealth failed to prove that [Petitioner] had the requisite mens rea for distribution.” Petition, p. 5. For the reasons set forth below, the Court finds that Petitioner’s representation at trial was Constitutionally adequate and will dismiss the Petition.

I. Procedural Background

Petitioner was represented at trial by Craig S. Cooley and Deborah D. Corcoran. Transcript of Trial, July 13, 2015 (“Tr. I”), 2. . . .

. . . .

A. Burden of proof and presumption

The petitioner in a writ of habeas corpus bears the burden of establishing his claim by the preponderance of the evidence. *E.g., Peyton v. Ellyson*, 207 Va. 423, 426, 150 S.E.2d 104, 107 (1966).

Courts reviewing counsel’s actions “must indulge a strong presumption that counsel’s conduct falls within the wide range of reasonable professional assistance.” *Shaikh v. Johnson*, 276 Va. 537, 544, 666 S.E.2d 325, 328 (2008) (quoting *Strickland v. Washington*, 466 U.S. 668, 689 (1984)).

. . . .

III. Petitioner’s Argument

Petitioner asserts that his counsels’ performance was Constitutionally deficient because they could have raised reasonable doubt as to the intent requirement for the distribution of child pornography charges if they had elicited from the defense experts certain testimony set forth in the Declarations attached to the Petition. Although the evidence showed that Petitioner knew Shareaza shared files from a specific “shared folder” location, Petitioner argues his counsel should have discovered and argued that there was no evidence he knew that “files that are in the process of being downloaded” could also be “available to other users.” Petition, ¶ 43.

In support of his claim, Petitioner includes declarations by his trial experts, Patrick J. Siewert and Larry Daniel. Mr. Siewert and Mr. Daniel, in identical language, state that if they had been asked, they would have testified that it is “somewhat complicated” for a user to choose not to share files

through a program such as Shareaza because “the software default is sharing.” Siewert Declaration, ¶4; Daniel Declaration, ¶4. Mr. Siewert and Mr. Daniel also set forth details about the nature of peer-to-peer file-sharing networks and how a user of Shareaza can inadvertently “share” a file while that user is in the process of downloading it, or even for a short while after a user has deleted it. Siewert Declaration, ¶6; Daniel Declaration, ¶6. In addition, Mr. Daniel goes on to assert that, “[b]ecause the files that were the subject of the distribution charges in this case were not found in a shared folder or on [Petitioner’s] computer, it appears that this [inadvertent sharing] is precisely what happened in this case.” Daniel Declaration, ¶7.

#### IV. Analysis

The question presented, therefore, is whether Petitioner’s counsels’ failure to elicit the specific testimony reflected in the Declarations “so undermined the proper functioning of the adversarial process that the trial cannot be relied on as having produced a just result.” *Strickland*, 466 U.S. at 686.

The Court cannot come to such a conclusion. The standard that Petitioner would have this Court adopt for counsel’s use of expert witnesses would place an unreasonable burden on counsel to possess the knowledge and insights that experts are retained to provide. Further, Petitioner cannot show a reasonable probability that, had his counsel elicited the testimony contained in the Declarations, the result of his proceeding would have been different.

##### A. Selection of Competent Expert Witnesses

The standard set forth by the United States Supreme Court in *Strickland*, that counsel’s representation be objectively reasonable, applies to all aspects of the representation, including the selection and use of expert witnesses. It is clear from the transcripts of the motions hearing and the trial that Petitioner’s counsel carefully chose and properly qualified the defense experts in order to support their trial strategy.

Patrick Siewert is “the principle [sic] consultant at Pro Digital Forensic Consulting[,]” a “full service digital forensic case intake, assessment, examinations, reporting, and expert witness service[.]” Transcript of Evidence July 14, 2015 (“Tr. II”) 163: 1 - 8. Mr. Siewert worked for various law enforcement agencies, including on an Internet Crimes Against Children Task Force; his training included courses at the “National Crime Center” and the “Federal Law Enforcement Training Center and the US Secret Service[.]” Tr. II, 163:10 - 164:2. His training includes “general behaviors of people who traffic in child pornography, as well as general behaviors of how they store those items on digital devices.” Transcript of Motions Hearing June 11, 2015 (“Tr. Hearing”), 70:7 - 10.

The other defense expert, Larry Daniel, is a “digital forensic examiner” with “over 200 hours of training in digital forensics” who holds

“six certifications” related to digital forensics and cellular data. Tr. Hearing, 33: 12 - 34: 11. Both experts teach digital forensics (Tr. Hearing, 37:8-18; Tr. II, 164:10-16), and Mr. Daniel wrote a book on digital forensics that was purchased by 115 libraries around the country, including the “FBI Library at Quantico.” Tr. Hearing, 36:2 - 37:7.

The Commonwealth stipulated to Mr. Daniel’s credentials as an expert in the area of storage of digital data (Tr. Hearing, 39:8- 40:1; Tr. II, 109:4 - 12) and Mr. Siewert was qualified as an expert “both as an ICAC [Internet Crimes Against Children] police agent and also as a computer forensic analyst.” Tr. Hearing, 73:19 - 22. The Commonwealth similarly stipulated Mr. Siewert’s credentials at trial. Tr. II, 162:8 -14.

The qualifications of Petitioner’s trial experts to deliver relevant testimony in cases involving the possession and distribution of electronic child pornography files are objectively reasonable. The court finds no basis for a finding of ineffective assistance of counsel based on counsels’ selection of expert witnesses.

#### B. Effective Use of Expert Witnesses

Having selected appropriate experts, it is next incumbent on counsel to make proper use of those experts. In their Declarations, Mr. Siewert and Mr. Daniel state that they “had no discussion with defense counsel about the legal or factual theory supporting the distribution charges in this case[.]” Siewert Declaration, ¶3; Daniel Declaration, ¶3.

The record reveals how the experts prepared for their testimony. Mr. Siewert testified that defense counsel contacted him to “assist with digital forensic examination of the evidence” in Petitioner’s case. Tr. Hearing, 74:17 - 75:1. He “forensically examine[d]” the three items of evidence introduced in the case (Tr. Hearing, 75:5 - 16) and reviewed the state police report. Tr. Hearing, 88: 19 - 20. Mr. Daniel testified that Petitioner’s counsel asked him “to review the reports” of the Commonwealth’s forensic expert, and to “review the evidence provided,” specifically, forensic copies of two computers and a memory card. Tr. Hearing, 109: 14 - 110: 13, 110:23 - 111 :2; Tr. II, 164: 17 - 165:10.

The experts state in their Declarations that “no one asked” them about the facts related to the distribution charge, and they “did not address it.” Siewert Declaration, ¶3; Daniel Declaration, ¶3. Knowing the nature of the charges against Petitioner, and having reviewed the evidence and reports, it is curious that the retained experts would not have shared any information they believed to be relevant to those charges. Both have prior law enforcement experience and could reasonably be inferred to know the basic elements of the crimes of possession and distribution of child pornography. Having reviewed the digital evidence and police reports, the experts can reasonably be inferred to also know the factual basis of the Commonwealth’s case.



Additionally, Petitioner's counsel seems to have taken reasonable steps in their use and preparation of the expert witnesses. Mr. Cooley asserts that he "met with and conferred with both of [Petitioner's] experts" and asked them to "suggest to us defenses or questions to use in cross examination." Letter from Craig Cooley to Rosemary V. Bourne, July 30, 2018, attached to the Commonwealth's Motion to Dismiss as Exhibit B ("Cooley Letter"), p. 1-2. Mr. Cooley maintains that neither expert suggested to him the potential defense of inadvertent sharing of the child pornography files, as they describe in their declarations, or any questions related to that issue. Cooley Letter, p. 2. Mr. Cooley acknowledges that he did not ask either expert about the "default" setting of Shareaza being to "share." Cooley Letter, p. 1.

It is not reasonable to expect Petitioner's counsel to have posed such a specific question. The better question, perhaps, is why did the experts not raise the issue with counsel? If the issue did not occur to them prior to trial, how can an attorney be expected to have known to ask about a subject that even the expert himself did not initially consider? If the experts did know about that potential line of defense, why did they not share it with Petitioner's counsel?

By stating that no one asked them about the distribution charge and so they did not address it, the experts are effectively asserting that they withheld information. Mr. Cooley, although an experienced criminal defense attorney, is not an expert in computer forensics. He is knowledgeable enough to know that he needed to associate experts, but he cannot be expected to know, in detail, all potentially relevant questions to ask.

An attorney has the right to reasonably rely on the input and opinions of their experts so long as the attorney has made available to qualified experts the information necessary for them to conduct the relevant analysis. To find otherwise would be to place on attorneys an affirmative obligation to essentially become experts themselves.

To require attorneys to ferret out all potentially relevant opinions is not reasonable, nor is it Constitutionally required. Even "[i]f counsel does not conduct a substantial investigation into each of several plausible lines of defense, assistance may nonetheless be effective." *Strickland*, at 681. An attorney must exercise competence in their selection of the expert and in making proper use of the information and opinions of such experts in support of a reasonable strategy. Petitioner's counsel did so. It is therefore necessary to determine whether the defense strategy of raising reasonable doubt that Petitioner was the person operating the computer was reasonable.

#### B. Reasonableness of counsels' trial strategy

Counsel's primary strategy at trial was to raise reasonable doubt based on there being "no evidence that [Petitioner] ever accessed or viewed" the child pornography files. Tr. I, 27:9-10. In support of his motion to strike the evidence on the distribution charges, Petitioner's counsel argued that even

the Commonwealth's expert "could not tell this court who turned on the share . . . and he absolutely had no evidence that suggested that this came from [Petitioner]." Tr. II, 247:8-14. Petitioner's counsel pointed out the "total absence of the identification of the distributor," raised the question of "whether there was a distribution" and analogized the Commonwealth's case to leaving lawn furniture outside and someone coming by and picking it up. Tr. II, 247:17-248:3. This strategy was at least partially successful; the Virginia Court of Appeals found the evidence insufficient to support two of the charges of possession of child pornography, second or subsequent offenses. *Kovach v. Commonwealth*, Va. Ct. Appeals Dec. 6, 2016 (Record No. 2013-15-2), p. 9.

Strategic choices by counsel about "which lines of defense to pursue are owed deference commensurate with the reasonableness of the professional judgments on which they are based." *Strickland* at 681. When reviewing whether counsel's strategic decisions were reasonable in light of the circumstances of the case, courts will look at "the experience of the attorney, the inconsistency of unpursued and pursued lines of defense, and the potential for prejudice from taking an unpursued line of defense." *Strickland*, at 681.

Petitioner's counsel are experienced criminal defense attorneys, each with many years of criminal defense experience. Evidence of their knowledge of facts, law and evidence is clearly shown in the transcripts of the proceedings.

The court cannot say that the unpursued line of defense of inadvertent sharing as proposed by Petitioner is entirely inconsistent with the chosen defense of raising reasonable doubt as to the identity of the person who accessed the child pornography files at all. However, arguing in the alternative that even if it was Petitioner who downloaded the files he did not know that he was sharing them would somewhat undermine the argument that it was not Petitioner who accessed them in the first place. This potential to undermine the chosen strategy also reflects the potential prejudice to the Petitioner from taking the unpursued line of defense; the strategy for which Petitioner advocates requires, to some degree, an acknowledgment that Petitioner was the one in control of the computer, and thus the downloading and subsequent sharing of the child pornography files. Petitioner's counsel's chosen line of defense was objectively reasonable given the circumstances of this case.

Further supporting the reasonableness of the chosen strategy, even if Petitioner's experts had shared the information contained in the experts' Declarations, is the Virginia Supreme Court case of *Kelley v. Commonwealth* (289 Va. 463, 771 S.E.2d 672 (2015)), decided a few months prior to Petitioner's trial. In *Kelley*, the Virginia Supreme Court explicitly rejected

the “inadvertent” or “accidental” distribution of child pornography theory in a case with remarkably similar facts.

The defendant in *Kelley* argued that evidence was insufficient to prove distribution of child pornography because “the peer-to-peer software he used to access and download child pornography *automatically* placed the child pornography files into a shared folder accessible to other users of the software.” *Kelley*, 289 Va. at 465, 771 S.E.2d at 672-73 (emphasis added). The defense expert in *Kelley* provided testimony remarkably similar to that which Petitioner maintains would have changed the outcome of his trial. In *Kelley*, the defense called an expert witness in computer forensics who testified that the software defendant used automatically downloaded files “into the shared folder unless the user chooses to place the files elsewhere to prevent sharing by other users.” *Kelley*, 289 Va. at 467, 771 S.E.2d at 674.

In affirming the conviction for distribution of child pornography, the Court noted that the entire purpose of peer-to-peer networks was to share files, so by merely “downloading the child pornography files into his shared folder, [the defendant] made the files available for sharing” with others, specifically the law enforcement officer who accessed the files. *Kelley*, 289 Va. at 468, 771 S.E.2d at 674.

As in *Kelley*, there is sufficient evidence in this case that Petitioner was familiar with the nature and functions of peer-to-peer file sharing networks. Initially, Petitioner denied any knowledge of any file sharing programs, then admitted to installing Shareaza (Tr. I, 111 : 18 - 112: 19), a program whose very name reveals its purpose to share files among the users of the network. Tr. I, 55: 17 - 21. Petitioner stated that he first installed Shareaza to download non-pornographic movies (Tr. I, 113:5-20) before admitting that he used it to download gay pornography featuring “younger guy[s].” Tr. I, 114:8-115:20. He also admitted that, on one occasion he “accidentally” downloaded child pornography. Tr. I, 116:8 - 117:6. Petitioner also admitted to using Shareaza and similar software, specifically Napster and Plex. Tr. I, 111:17 - 112:10.

The Court of Appeals relied on these facts and on *Kelley* to uphold Petitioner’s distribution convictions on his direct appeal. *Kovach v. Commonwealth*, Va. Ct. Appeals Dec. 6, 2016 (Record No. 2013-15-2). The court held that “it was reasonable for the factfinder to conclude that appellant should have known that the software had the ability to share files with other users” merely on the basis that Petitioner “knowingly downloaded and used peer-to-peer sharing software . . . admitted to downloading movies and adult pornography” and that he had “accidentally downloaded child pornography in the past.” *Kovach v. Commonwealth*, Va. Ct. Appeals Dec. 6, 2016 (Record No. 2013-15-2), p. 9-10. The information set forth in the Declarations would not have changed these facts. In *Kelley*, as here, it is

immaterial that the software setting which allowed for the distribution of the child pornography was “automatic”, or as Petitioner describes, “default.”

Counsels’ strategic decision in this case was based on reasonable assumptions based on the totality of the circumstances. Pursuant to *Kelley*, Petitioner’s statements provided sufficient evidence to defeat the Petitioner’s proposed “inadvertent” sharing defense. Having chosen a reasonable strategy given the circumstances of the case, counsel had no obligation to “investigate lines of defense that he has chosen not to employ at trial.” *Strickland* at 681 (citation and internal quotations omitted).

D. Prejudice prong of Strickland analysis

Having found counsels’ actions to be objectively reasonable, the court need not address the second prong of the *Strickland* analysis, prejudice to Petitioner’s case. *Shaikh*, 276 Va. at 544, 666 S.E.2d at 328 (citing *Strickland*, at 697) (other citations omitted) (“[a] reviewing court does not need to address” the prejudice prong of the *Strickland* analysis where a petitioner “fails to make a sufficient showing” that counsel’s assistance was ineffective). Nonetheless, the *Kelley* decision so directly impacts the determination of any potential prejudice to Petitioner’s case that it warrants some analysis.

Even assuming that Petitioner’s counsels’ strategic decisions were unreasonable, Petitioner cannot show that there is a reasonable probability that, “but for counsel’s unprofessional errors, the result of the proceeding would have been different.” *Strickland*, 466 U.S. at 694; *Shaikh*, 276 Va. at 544, 666 S.E.2d at 328 (other citations omitted). Because of the similarity of the facts between Petitioner’s case and the *Kelley* case, it is not credible that Petitioner’s proposed strategy would have changed the outcome of his trial. Finally, it is worth noting the fact that a user of Shareaza could inadvertently share files was not contested during Petitioner’s trial, and was in fact brought out by the Commonwealth’s own expert witness. On cross examination, Special Agent Mike Jedry of the Virginia State Police acknowledged that a user could “accidentally” share files, and that he was aware of cases where individuals who were not familiar with the way file sharing worked did not realize that the program was sharing. Tr. I, pp. 124 - 126. The trial court was clearly made aware of the fact that it was possible to share files on Shareaza accidentally. It just as clearly rejected that as sufficient to establish reasonable doubt, just as the Virginia Supreme Court did in *Kelley* and the Court of Appeals did in Petitioner’s direct appeal. The compelling evidence of Petitioner’s knowledge of Shareaza and file sharing software generally mean that, in light of *Kelley*, Petitioner cannot satisfy his burden to show that he suffered any prejudice, even if his counsel should have elicited the proposed expert testimony.

## V. Conclusion

To prevail on his claim of ineffective assistance of counsel, the burden is on the Petitioner to show by a preponderance of the evidence both that his counsels' performance was Constitutionally deficient and that he suffered prejudice as a result of the deficient representation. When viewed in light of the transcripts of proceedings and the filings in this Petition, it is clear that Petitioner has failed to show that his counsels' performance was ineffective; even assuming there was some deficiency, the Petitioner fails to make a showing that he reasonably could have suffered any prejudice as a result. Accordingly, the Court holds that Petitioner's ineffective assistance of counsel claim fails and his Petition is DENIED.

(ECF No. 1-1 at 12–21 (alterations in original).)

Kovach insists that the Circuit Court's rejection of his claim is erroneous because:

The evidence viewed in the light most favorable to the Commonwealth showed that Kovach admitted he used the file sharing program, but stated he used it to download movies and gay pornography. Kovach denied any intent to download child pornography. Agent Jedrey testified that sharing could be unintentionally turned on. Users can be unfamiliar with sharing and whether it is occurring and using the software without knowing they are sharing. Of the files Jedrey downloaded, some were unrelated to child pornography. Key here is that none of the files downloaded and forming the basis for the distribution charges were found either in a shared folder or on any devices seized from Kovach's home. Jedrey testified that Kovach denied preserving any child pornography and always deleted any files downloaded that appeared inappropriate.

Defense counsel defended the distribution charges by arguing that there was no proof that Kovach was the one using the peer-to-peer software and no proof that Kovach was the person who turned the sharing capability "on."

But defense counsel failed to realize and defend Kovach by arguing that even if the trial court found beyond a reasonable doubt that Kovach had controlled the peer-to-peer software, there was no evidence of intent to distribute because *none of the files that were the subject of the distribution charges were found in an accessible shared folder on Kovach's devices.*

Trial counsel in this case never discussed with their experts the legal theory of passive distribution because they did not understand it. And so they never consulted with their experts about the factual bases for the distribution charges in this case.

If trial counsel had consulted with their experts, they would have discovered that not only is "sharing" the default of Shareaza software, but it



is complicated to turn-off. They also would have discovered that *Shareaza makes files that are in the process of being downloaded available to other users* – that is– the detective can obtain the files from a computer, but the owner of that computer would not be liable for distribution.

While the evidence was sufficient to find that Kovach possessed child pornography, the evidence was insufficient to find that Kovach had the requisite *mens rea*, either intent or knowledge, to distribute child pornography.

(ECF No. 1 ¶¶ 46–51 (paragraph numbers omitted) (citation omitted).)

The Circuit Court was well aware that sharing was the default setting for Shareaza, and that people sometimes are unaware that the program is sharing. These facts were emphasized to the judge in following exchange with Special Agent Jedry.

Q. And you have done this for a while. There are certainly situations where people have either failed to cut off the Share button, I’m going to call it a button, but whatever it is that allows you to share, but you have certainly come across cases where people just didn’t realize they had it on, or it was on from the beginning and they never know how to cut it off?

A. Yeah, there were people that weren’t familiar with the way the file sharing worked and didn’t realize it was operationally sharing.

(July 13, 2015 Tr. 126.)

Equally unconvincing is Kovach’s suggestion that he was ignorant that he was sharing child pornography. The evidence at trial reflected that the very purpose of peer-to-peer file sharing programs, such as Shareaza, “is that everyone that is on that network shares their files.” (July 13, 2015 Tr. 55.) Additionally, Kovach informed the investigators that he used the internet for file sharing and specifically mentioned Shareaza as the file sharing program that he used. (July 13, 2015 Tr. 109, 111–12.)

Furthermore, Kovach suggests that counsel should have pressed the argument that Kovach inadvertently began downloading some child pornography using Shareaza and

then Shareaza shared those images with Special Agent Jedry, while the images were still downloading, before Kovach discovered images that contained child pornography. The notion that Kovach's downloading and sharing of the child pornography was inadvertent is specious. The evidence reflected that Shareaza would search for available files depending on the topic you typed into "the search box." (July 13, 2015 Tr. 131.)<sup>8</sup> Shareaza then "is going to give you several responses, so it is going to say, hey, you have these files to choose from, but it is not going to download those files for you." (July 13, 2015 Tr. 131.) The user would then have to select which files he or she would like to download. (July 13, 2015 Tr. 131.)

Kovach told investigators here that if he downloaded child pornography, he did so inadvertently and immediately deleted it. That statement is simply not credible given the evidence of child pornography found on the devices in the residence and the names of the child pornography files Special Agent Jedrey obtained from Kovach via Shareaza. The file names Kovach had selected to download on his computer and that were available to Special Agent Jedrey were titled: "PTHC, Boy 8YO Sucked by His Mom, and Boy Plus Man"; "11YO Boy Gets a Real Blow Job," and "Andy's Brother PTHC PO Gay.MPG." (July 13, 2015 Tr. 62.)<sup>9</sup>

Lastly, Kovach makes much of the fact that none of the images that were the subject of the distribution of child pornography charges were found in an accessible

---

<sup>8</sup> Kovach employed such search terms as: "P 101," "boy man," and "boy pics." (July 14, 2015 Tr. 60.) P 101 is a search term used for child pornography. (July 14, 2015 Tr. 60.)

<sup>9</sup> "P-T-H-C stands for preteen hardcore." (July 13, 2015 Tr. 60.)

shared folder on Kovach's devices. A couple of months had elapsed between that last time Special Agent Jedry obtained child pornography from Kovach's computer with the Shareaza program and before the police searched his home and seized his devices. That window of time provided ample opportunity for Kovach to dispose of any illicit electronic files or even devices containing child pornography. The evidence suggested that is exactly what happened in this case. Kovach had moved or removed other child pornography files from his desktop computer so that videos or pictures were no longer recoverable. (July 14, 2015 Tr. 43–46.)<sup>10</sup> Furthermore, there was evidence that a four gigabyte SD card had been used on Kovach's computer and that four gigabyte SD card was not been recovered by the police. (July 14, 2015 Tr. 186.) Finally, child pornography files that Special Agent Jedrey viewed or downloaded from Kovach's IP address had been downloaded onto Kovach's SD card. (July 14, 2015 Tr. 46.) All of these circumstances bolster the Circuit Court's conclusion that Kovach was not prejudiced by any omission of counsel.

In light of this record, the Court discerns no unreasonable application of the law and no unreasonable determination of the facts in the Circuit Court's rejection of Kovach's claim. *See* 28 U.S.C. § 2254 (d)(1)–(2).

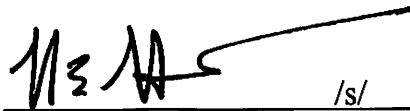
---

<sup>10</sup> As noted by the Court of Appeals of Virginia, “several of the videos that Special Agent Jedrey obtained while he was using peer-to-peer sharing software were also found on the SD card in appellant's hamper.” *Kovach v. Commonwealth*, No. 2013–15–2, 2016 WL 7094215, at \*5 (Va. Ct. App. Dec. 6, 2016).

#### IV. CONCLUSION

Kovach's claim will be dismissed. The Amended Motion to Dismiss (ECF No. 10) will be granted. The § 2254 Petition will be denied. The action will be dismissed. A certificate of appealability will be denied.

An appropriate Order will accompany this Memorandum Opinion.

A handwritten signature in black ink, appearing to read 'H. Hudson', is written over a horizontal line. To the right of the signature, the text '/s/' is printed.

Henry E. Hudson  
Senior United States District Judge

Date: May 30, 2023  
Richmond, Virginia